

REMARKS

Status of the Application:

Claims 1–3, 5–9 and 11–29 are the claims of record of the application. Claims 1–3, 5–9 and 11–29 have been finally rejected.

This is also a Request for Continued Examination

Applicants Request Continued Examination under 37 CFR 1.114. The associated fee is included.

Interview held May 17, 2007

Applicants appreciate the courtesy shown during the telephone interview held May 17, 2007 between the Examiner, the Supervising Examiner, and the undersigned. The claims and the prior art were discussed. There was agreement reached that amending the claims to include, as an example, to claim 1, the step of managing access points including configuring one or more configuration parameters (other than the BSSID of the AP), and further describing that the AP database included not only the service set identifier of each managed AP, but in addition configuration parameters, and that ascertaining if a potential rogue AP is a managed AP includes matching more than the BSSID in the AP database would lead to a further search of the cited prior art to ascertain if the elements of the claim as amended are taught.

Amendment to the Claims:

Using claim 1 as an example, Applicants have amended the claims to add, for example, to claim 1 the step of managing managed access points (APs), including carrying out one or both of power control and frequency selection to configure one or more configuration parameters of the managed access points. This is disclosed, for example, in paragraph [0061].

Claim 1 also was amended to state that the AP database includes for each managed AP, the service set identifier of the managed AP and one or more of the configuration parameters. This is disclosed, for example, in [0087].

Claim 1 also was amended to clarify that the reports about the potential rogue AP sent by a managed AP include detection information, and information on the any beacon or probe response received. The detection information includes the service set identifier of the potential rogue AP, and at least one further item of information, and the information on the received beacon or probe response includes at least the service set identifier in the beacon or probe response, and one or more configuration parameters. This is disclosed, for example, in paragraphs [0063] to [0073].

Claim 1 also was amended to state that ascertaining if the potential rogue AP is a managed AP includes:

ascertaining if there is a match for the service set identifier of the potential rogue AP in the AP database, and if there is a match for one or more configuration parameters of the potential rogue AP in the AP database in addition to the service set identifier of the potential rogue AP,

such that at least a plurality of parameters are matched in the AP database to ascertain whether a potential rogue AP is a managed AP.

This is disclosed, for example, in [0092].

New claim 30 states that the information stored in the AP database on each managed AP includes a maximum power setting or a frequency setting or both a maximum power and a frequency setting. See, e.g., paragraph [0087].

New claim 31 states that the detection information includes at least the channel the detected AP's beacon or probe response was received on, and wherein the information on the received beacon or probe response includes at least a service set identifier in the beacon or probe response. See, e.g., paragraphs [0064 to 0073].

New claim 32 adds the feature of sending a scan request to one or more managed APs of the wireless network including a request for the receiving managed AP to request the AP's clients to scan for beacons and probe responses. This was in the prior version of claim 1, which has now been simplified to remove this feature.

The other independent claims have similarly been amended to be consistent, and new claims added to in similar manner to how claims 30–32 were added.

For the convenience of the examiner, an Appendix containing a clean listing of the claims after this amendment is provided.

Discussion

In the final office action, claims 1–3, 6–9, 11–29 were rejected under 35 USC 103(a) as being unpatentable over FUJII et al. (US PGPUB 2003/0117985 A1) in view of Whelan et al. (US PGPUB 2004/0003285 A1).

In that final office action, the Examiner has cited FUJII et al.'s BSSID, that is, the potential rogue AP's service set identifier as “configuration information.”

Applicants assert that the present invention as stated in amended claim 1 includes features not found in the cited prior art or combinations thereof.

Specifically, the cited prior art does not disclose a central management entity managing of the APs by carrying out power control or frequency selection to configure configuration parameters.

The present invention uses the fact that there is a central management entity that sets configuration parameters, and therefore knows the parameters, in order to use this information **in addition to the service set identifier of the potential rogue AP** in order to ascertain whether the potential rogue AP is a managed AP. In previous versions of the claims, the Applicants refer to this as "configuration information," and the examiner had cited Fujii's BSSID, that is, the potential rogue AP's service set identifier as such configuration information. Applicants respectfully disagree that the BSSID, e.g., the MAC address of a potential rogue is "configuration information." However, in order to reach agreement, the claims have been amended to state:

- 1) Applicants' AP database includes for each managed AP, the service set identifier of the managed AP and one or more of the configuration parameters.
- 2) The information sent from an AP that detected a beacon or probe response from a potential rogue AP (a) detection information, and (b) information on the beacon or probe response received. The detection information includes the service set identifier of the potential rogue AP, and at least one further item of information. The information on the received beacon or probe response including at least the service set identifier in the beacon or probe response, and one or more configuration parameters.
- 3) Ascertaining if a potential rogue AP is a managed AP includes ascertaining there is a match for the service set identifier of the potential rogue AP in the AP database, and if there is a match for one or more configuration parameters of the potential rogue AP in the AP database **in addition to the service set identifier of the potential rogue AP**.

Thus, at least a plurality of parameters are matched in the AP database to ascertain whether a potential rogue AP is a managed AP. That is, a multi-parameter signature is used in the matching of information received about a potential rogue with information in the AP database.

These features are not disclosed in the cited prior art.

Newly added dependent claims 30 and 31 add to what specific parameters are in some disclosed embodiments.

Independent claim 18 is a method claim that described a method at one of the managed APs, and has been amended to include the features and limitations described above.

Independent claim 18 is a method claim that described a method at one of the managed APs, and has been amended to include the features and limitations described above.

Independent claim 26 is for a computer-readable medium encoded with computer readable instructions that when executed cause one or more processors of a processing system to execute a method. The method includes the features and limitations recited in claim 1.

Independent claim 27 is for a computer-readable medium encoded with computer readable instructions that when executed cause one or more processors of a processing system to execute a method. The method includes the features and limitations recited in claim 18.

Independent claim 28 is for an apparatus that includes a processing system and a tangible medium storing an AP database. The processing system is programmed to carry out a process that includes features and limitations recited in claim 1.

Independent claim 29 is for an apparatus that includes a processing system programmed to carry out a process that includes features and limitations recited in claim 18.

The above argument for claim 1 applies to each of these independent claims, appropriately modified to the type of claim, and is incorporated herein.

The rejection of the independent claims under 35 USC 103 is therefore believed overcome.

Applicant also has amended claim 13 to add that the detection information includes absolute RSSI information, as disclosed in specification. Thus, even if Examiner remains unconvinced by Applicant's arguments for the independent claims, Examiner's rejections of some of the dependent claims under 35 USC 103(a) are also believed overcome.

For these reasons, and in view of the above amendment, this application is now considered to be in condition for allowance and such action is earnestly solicited.

Conclusion

The Applicants believe all of Examiner's rejections have been overcome with respect to all remaining claims (as amended), and that the remaining claims are allowable. Action to that end is respectfully requested.

If the Examiner has any questions or comments that would advance the prosecution and allowance of this application, an email message to the undersigned at dov@inventek.com, or a telephone call to the undersigned at +1-510-547-3378 is requested.

Respectfully Submitted,

May 21, 2007

Date

/Dov Rosenfeld/ #38687

Dov Rosenfeld, Reg. No. 38687

Address for correspondence:

Dov Rosenfeld
5507 College Avenue, Suite 2,
Oakland, CA 94618
Tel. 510-547-3378
Fax: +1-510-291-2985
Email: dov@inventek.com